United Nations A/64/422/Add.3

General Assembly

Distr.: General
15 December 2009

Original: English

Sixty-fourth session
Agenda item 55 (c)

Globalization and interdependence: science and technology for development

Report of the Second Committee*

Rapporteur: Ms. Denise **McQuade** (Ireland)

I. Introduction

1. The Second Committee held a substantive debate on agenda item 55 (see A/64/422, para. 2). Action on sub-item (c) was taken at the 30th, 33rd, 37th and 38th meetings, on 3, 10 and 25 November and 1 December 2009. An account of the Committee's consideration of the sub-item is contained in the relevant summary records (A/C.2/64/SR.30, 33, 37 and 38).

II. Consideration of draft resolutions

A. Draft resolutions A/C.2/64/L.8 and Rev.1

2. At the 30th meeting, on 3 November, the representative of the United States of America, on behalf of Australia, Bulgaria, Canada, Estonia, Israel, Japan, the Marshall Islands, the Republic of Korea and the United Kingdom of Great Britain and Northern Ireland, introduced a draft resolution entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures" (A/C.2/64/L.8), which read:

> "*The General Assembly*,
>
> "*Recalling* its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity and 58/199 of 23 December 2003 on the creation of a global

* The report of the Committee on this item is being issued in four parts, under the symbol A/64/422 and Add.1-3.

09-64946 (E) 181209

Please recycle

culture of cybersecurity and the protection of critical information infrastructures,

"*Recalling also* its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008 on developments in the field of information and telecommunications in the context of international security,

"*Recalling further* the outcomes of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November (second phase), in which States recognized that freedom of expression and the free flow of information, ideas and knowledge are essential for today's information society and beneficial to development, and that, because confidence and security in the use of information and communications technologies are among the main pillars of the information society, a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented,

"*Recognizing* the increasingly indispensable contribution made by networked information technologies to most of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals, organizations and Governments,

"*Noting* that Governments, businesses, civil society and individuals are increasingly reliant upon a global network of information infrastructures, and that such reliance will only increase,

"*Noting also* that gaps in access to and the use of information technologies by States can diminish their social and economic prosperity, and noting especially the needs of less developed countries in the areas of cybersecurity best practices and training,

"*Expressing concern* that threats to the reliable functioning of critical information infrastructures and to the integrity of the information carried over those networks are growing in both sophistication and gravity, affecting domestic, national and international welfare,

"*Affirming* that the security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles,

"*Recognizing* that national efforts should be supported by national, regional and international information-sharing and collaboration, so as to confront effectively the increasingly transnational nature of such threats,

"*Noting* the work of relevant regional and international organizations on enhancing cybersecurity, especially those that have encouraged national efforts and have fostered international cooperation,

"*Noting also* the 2009 report of the International Telecommunication Union entitled 'Securing information and communication networks: best practices for developing a culture of cybersecurity', which focused on a comprehensive national approach to cybersecurity consistent with free speech, the free flow of information and due process of law,

"*Recognizing* that national efforts to protect critical information infrastructures benefit from a periodic assessment of their progress,

"1. *Invites* Member States to provide, on a voluntary basis, summaries of their key initiatives on cybersecurity and the protection of critical information infrastructures, so as to highlight national achievements and best practices, lessons learned and areas for further action;

"2. *Offers* Members States, in this regard, the attached national cybersecurity self-assessment survey as a possible tool to aid them, where appropriate, in reviewing national efforts on cybersecurity and the protection of critical information infrastructures;

"3. *Invites* all Member States that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to inform the Secretary-General, by the sixty-fifth session of the General Assembly, of best practices and measures that could assist other Member States, regional and international organizations, private-sector and civil society stakeholders in their efforts to create a global culture of cybersecurity.

"Annex

"Self-assessment tool for national efforts to protect critical information infrastructures

"*Taking stock of cybersecurity needs and strategies*

"1. Evaluate the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

"2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.

"3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present, and the current management plan; note how changes in economic environment, national security priorities and civil society needs affect these calculations.

"4. Determine the goals of your national cybersecurity and critical information infrastructure protection strategy, describe its goals, current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives, and how such a strategy fits within regional and international initiatives.

"*Stakeholder roles and responsibilities*

"5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

- "• National Government ministries or agencies, noting primary points of contact and responsibilities of each;
- "• Other government (local and regional) participants;
- "• Non-government actors, including industry, civil society and academia;
- "• Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

"*Policy processes and participation*

"6. Identify formal and informal venues that currently exist for Government-industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and its adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

"7. Identify forums or structures that may further be needed to integrate the Government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

"*Public-private cooperation*

"8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information-sharing and incident management.

"9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

"*Incident management and recovery*

"10. Identify the agency in your Government that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

"11. Separately, identify your national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing

tools and procedures for the dissemination of incident-management information.

"12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

"*Legal frameworks*

"13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communication technologies, and use regional and international conventions, arrangements and precedents in these reviews. Determine whether your State is a party to, or plans to accede to the Budapest Convention on Cybercrime, or plans to adopt commensurate laws.

"14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

"15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

"16. Examine whether your State participates in international efforts to combat cybercrime, such as the 24/7 Cybercrime Point of Contact Network, and determine to what extent doing so would further national cybersecurity goals.

"17. Determine the requirements for your national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in your national territory, but victims reside elsewhere.

"*Developing a global culture of cybersecurity*

"18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in United Nations General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements."

3. At its 37th meeting, on 25 November, the Committee had before it a revised draft resolution entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures" (A/C.2/64/L.8/Rev.1), submitted by the United States, on behalf of Antigua and Barbuda, Argentina, Australia, Belize, Bulgaria, Canada, Chile, Croatia, the Dominican Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Israel, Italy, Japan, Latvia, the Marshall Islands, Mexico, Montenegro, Nigeria, Panama,

Poland, Portugal, the Republic of Korea, the Republic of Moldova, Romania, Singapore, Slovenia, Spain, Sweden, Ukraine and the United Kingdom of Great Britain and Northern Ireland.

4. At the same meeting, the Committee was informed that the revised draft resolution had no programme budget implications.

5. Also at the same meeting, the representative of the United States orally corrected the draft resolution.

6. Also at the 37th meeting, Greece, India, Jamaica and Lithuania joined in sponsoring the draft resolution.

7. The Committee adopted draft resolution A/C.2/64/L.8/Rev.1, as orally corrected (see para. 14, draft resolution I).

B. Draft resolutions A/C.2/64/L.17 and A/C.2/64/L.49

8. At the 33rd meeting, on 10 November, the representative of the Sudan, on behalf of the States Members of the United Nations that are members of the Group of 77 and China, introduced a draft resolution entitled "Science and technology for development" (A/C.2/64/L.17), which read:

"*The General Assembly*,

"*Recalling* its resolutions 58/200 of 23 December 2003, 59/220 of 22 December 2004, 60/205 of 22 December 2005 and 62/201 of 19 December 2007,

"*Recalling also* its resolution 61/207 of 20 December 2006 and its reference to science and technology,

"*Recalling further* Economic and Social Council resolution 2006/46 of 28 July 2006,

"*Recognizing* the vital role that science and technology, including environmentally sound technologies, can play in development and in facilitating efforts to eradicate poverty, achieve food security, fight diseases, improve education, protect the environment, accelerate the pace of economic diversification and transformation and improve productivity and competitiveness,

"*Recalling* the 2005 World Summit Outcome,

"*Recalling also* the outcomes of the World Summit on the Information Society,

"*Recognizing* that international support can help developing countries to benefit from technological advances and can enhance their productive capacity,

"*Underscoring* the role that traditional knowledge can play in technological development, and in the sustainable management and use of natural resources,

"*Acknowledging* the urgent need to bridge the digital divide and to assist developing countries in accessing the potential benefits of information and communications technologies,

"*Welcoming* the adoption of the Bali Strategic Plan for Technology Support and Capacity-building of the United Nations Environment Programme,

"*Reaffirming* the need to enhance the science and technology programmes of the relevant entities of the United Nations system,

"*Noting with appreciation* the collaboration between the Commission on Science and Technology for Development and the United Nations Conference on Trade and Development in establishing a network of centres of excellence in science and technology for developing countries and in designing and carrying out science, technology and innovation policy reviews,

"*Taking note with interest* of the establishment of the inter-agency cooperation network on biotechnology, UN-Biotech, as described in the report of the Secretary-General on science and technology for development,

"*Taking note* of the report of the Secretary-General,

"*Taking note also* of Economic and Social Council resolution 2009/8 of 24 July 2009 on science and technology for development,

"1. *Reaffirms* its commitment:

"(a) To strengthen and enhance existing mechanisms and to support initiatives for research and development, including through voluntary partnerships between the public and private sectors, to address the special needs of developing countries in the areas of health, agriculture, conservation, sustainable use of natural resources and environmental management, energy, forestry and the impact of climate change;

"(b) To promote and facilitate, as appropriate, access to, and development, transfer and diffusion of, technologies, including environmentally sound technologies and the corresponding know-how, to developing countries;

"(c) To assist developing countries in their efforts to promote and develop national strategies for human resources and science and technology, which are primary drivers of national capacity-building for development;

"(d) To promote and support greater efforts to develop the technology for renewable sources of energy, such as solar, biomass, hydro, wind and geothermal energy;

"(e) To implement policies at the national and international levels to attract both public and private investment, domestic and foreign, that enhances knowledge, transfers technology on mutually agreed terms and raises productivity;

"(f) To support the efforts of developing countries, individually and collectively, to harness new agricultural technologies in order to increase agricultural productivity through environmentally sustainable means;

"2. *Recognizes* that science and technology, including information and communications technologies, are vital for the achievement of internationally agreed development goals, including the Millennium Development Goals, and for the full participation of developing countries in the global economy;

"3. *Requests* the Commission on Science and Technology for Development to provide a forum within which to continue to assist the Economic and Social Council as the focal point in the system-wide follow-up to the outcomes of the World Summit on the Information Society and to address within its mandate, in accordance with Council resolution 2006/46, the special needs of developing countries in areas such as agriculture, rural development, information and communications technologies and environmental management;

"4. *Encourages* the United Nations Conference on Trade and Development, in collaboration with relevant partners, to continue to undertake science, technology and innovation policy reviews, with a view to assisting developing countries and countries with economies in transition in identifying the measures that are needed to integrate science, technology and innovation policies into their national development strategies;

"5. *Encourages* the United Nations Conference on Trade and Development and other relevant organizations to assist developing countries in their efforts to integrate science, technology and innovation policies in national development strategies;

"6. *Encourages* Governments to strengthen and foster investment in research and development for environmentally sound technologies and to promote the involvement of the business and financial sectors in the development of those technologies, and invites the international community to support those efforts;

"7. *Encourages* existing arrangements and the further promotion of regional, subregional and interregional joint research and development projects by, where feasible, mobilizing existing scientific and research and development resources and by networking sophisticated scientific facilities and research equipment;

"8. *Encourages* the international community to continue to facilitate, in view of the difference in level of development between countries, an adequate diffusion of scientific and technical knowledge and transfer of, access to, and acquisition of technology for developing countries, under fair, transparent and mutually agreed terms, in a manner conducive to social and economic welfare for the benefit of society;

"9. *Calls for* continued collaboration between United Nations entities and other international organizations, civil society and the private sector in implementing the outcomes of the World Summit on the Information Society, with a view to putting the potential of information and communications technologies at the service of development through policy research on the digital divide and on new challenges of the information society, as well as technical assistance activities, involving multi-stakeholder partnerships;

"10. *Requests* the Secretary-General to submit to the General Assembly at its sixty-sixth session a report on the implementation of the present resolution and recommendations for future follow-up, including lessons learned in integrating science, technology and innovation policies into national development strategies."

9. At its 38th meeting, on 1 December, the Committee had before it a draft resolution entitled "Science and technology for development" (A/C.2/64/L.49), submitted by the Vice-Chairperson of the Committee, Mohamed Cherif Diallo (Guinea), on the basis of informal consultations held on draft resolution A/C.2/64/L.17.

10. At the same meeting, upon the proposal of the Chairperson, the Committee agreed to waive the relevant provision of rule 120 of the rules of procedure of the General Assembly and proceeded to take action on draft resolution A/C.2/64/L.49.

11. Also at the same meeting, the Committee was informed that draft resolution A/C.2/64/L.49 contained no programme budget implications.

12. Also at the 38th meeting, the Committee adopted draft resolution A/C.2/64/L.49 (see para. 14, draft resolution II).

13. In the light of the adoption of draft resolution A/C.2/64/L.49, draft resolution A/C.2/64/L.17 was withdrawn by its sponsors.

III. Recommendations of the Second Committee

14. The Second Committee recommends to the General Assembly the adoption of the following draft resolutions:

Draft resolution I
Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

The General Assembly,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity and 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008 on developments with respect to information technologies in the context of international security,

Recalling further the outcomes of the World Summit on the Information Society, held in 2003 (first phase) and in 2005 (second phase),[1]

Recognizing that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented,

Recognizing also the increasing contribution made by networked information technologies to many of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals and organizations, Governments, business and civil society,

Recognizing further that, in a manner appropriate to their roles, Governments, business, other organizations and individual owners and users of information technologies must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing the importance of the mandate of the Internet Governance Forum as a multi-stakeholder dialogue to discuss various matters, including, inter alia, public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet, and reiterating that all Governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet,

[1] See A/C.2/59/3 and A/60/687.

Reaffirming the continuing need to enhance cooperation, to enable Governments, on an equal footing, to carry out their roles and responsibilities in international public policy issues pertaining to the Internet, but not the day-to-day technical and operational matters that do not impact on international public policy issues,

Recognizing that each country will determine its own critical information infrastructures,

Reaffirming the need to harness the potential of information and communications technologies to promote the achievement of the internationally agreed development goals, including the Millennium Development Goals, recognizing that gaps in access to and use of information technologies by States can diminish their economic prosperity, and reaffirming also the effectiveness of cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity,

Stressing the need for enhanced efforts to close the digital divide in order to achieve universal access to information and communication technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing countries, especially the least developed countries, in the area of cybersecurity best practices and training,

Expressing concern that threats to the reliable functioning of critical information infrastructures and to the integrity of the information carried over those networks are growing in both sophistication and gravity, affecting domestic, national and international welfare,

Affirming that the security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles,

Recognizing that national efforts should be supported by international information-sharing and collaboration, so as to effectively confront the increasingly transnational nature of such threats,

Noting the work of relevant regional and international organizations on enhancing cybersecurity, and reiterating their role in encouraging national efforts and fostering international cooperation,

Noting also the 2009 report of the International Telecommunication Union on securing information and communication networks: best practices for developing a culture of cybersecurity, which focused on a comprehensive national approach to cybersecurity consistent with free speech, the free flow of information and due process of law,

Recognizing that national efforts to protect critical information infrastructures benefit from a periodic assessment of their progress,

1. *Invites* Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts to protect their critical information infrastructures and strengthen their cybersecurity, so as to

highlight areas for further action, with the goal of increasing the global culture of cybersecurity;

2. *Encourages* Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity by providing such information to the Secretary-General for compilation and dissemination to Member States.

Annex

Voluntary self-assessment tool for national efforts to protect critical information infrastructures[2]

Taking stock of cybersecurity needs and strategies

1. Assess the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.

3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present and the current management plan; note how changes in the economic environment, national security priorities and civil society needs affect these calculations.

4. Determine the goals of the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives and how such a strategy fits within regional and international initiatives.

Stakeholder roles and responsibilities

5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

- National Government ministries or agencies, noting primary points of contact and responsibilities of each;
- Other government (local and regional) participants;
- Non-governmental actors, including industry, civil society and academia;
- Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

[2] This is a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity.

Policy processes and participation

6. Identify formal and informal venues that currently exist for Government-industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

7. Identify forums or structures that may further be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

Public-private cooperation

8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information-sharing and incident management.

9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

Incident management and recovery

10. Identify the Government agency that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

11. Separately, identify national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident-management information.

12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

Legal frameworks

13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

Developing a global culture of cybersecurity

18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.

Draft resolution II
Science and technology for development

The General Assembly,

Recalling its resolutions 58/200 of 23 December 2003, 59/220 of 22 December 2004, 60/205 of 22 December 2005 and 62/201 of 19 December 2007,

Recalling also its resolution 61/207 of 20 December 2006 and its reference to science and technology,

Taking note of Economic and Social Council resolutions 2006/46 of 28 July 2006 and 2009/8 of 24 July 2009,

Recognizing the vital role that science and technology, including environmentally sound technologies, can play in development and in facilitating efforts to eradicate poverty, achieve food security, fight diseases, improve education, protect the environment, accelerate the pace of economic diversification and transformation and improve productivity and competitiveness,

Recalling the 2005 World Summit Outcome,[1]

Recalling also the outcomes of the World Summit on the Information Society,[2]

Recognizing that international support can help developing countries to benefit from technological advances and can enhance their productive capacity,

Underscoring the role that traditional knowledge can play in technological development, and in the sustainable management and use of natural resources,

Acknowledging the urgent need to bridge the digital divide and to assist developing countries in accessing the potential benefits of information and communications technologies,

Encouraging continued efforts towards the implementation of the Bali Strategic Plan for Technology Support and Capacity-building of the United Nations Environment Programme,[3]

Reaffirming the need to enhance the science and technology programmes of the relevant entities of the United Nations system,

Noting with appreciation the collaboration between the Commission on Science and Technology for Development and the United Nations Conference on Trade and Development in establishing a network of centres of excellence in science and technology for developing countries and in designing and carrying out science, technology and innovation policy reviews,

Taking note with interest of the establishment of the inter-agency cooperation network on biotechnology, UN-Biotech, as described in the report of the Secretary-General on science and technology for development,[4]

Taking note of the report of the Secretary-General,

---

[1] See resolution 60/1.

[2] See A/60/687 and A/C.2/59/3, annex, chap. I.

[3] UNEP/GC.23/6/Add.1 and Corr.1, annex.

[4] A/64/168.

Encouraging the development of initiatives to promote private sector engagement in technology transfer and technological and scientific cooperation,

1. *Reaffirms its commitment*:

(a) To strengthen and enhance existing mechanisms and to support initiatives for research and development, including through voluntary partnerships between the public and private sectors, to address the special needs of developing countries in the areas of health, agriculture, conservation, sustainable use of natural resources and environmental management, energy, forestry and the impact of climate change;

(b) To promote and facilitate, as appropriate, access to, and development, transfer and diffusion of, technologies, including environmentally sound technologies and the corresponding know-how, to developing countries;

(c) To assist developing countries in their efforts to promote and develop national strategies for human resources and science and technology, which are primary drivers of national capacity-building for development;

(d) To promote and support greater efforts to develop renewable sources of energy, including appropriate technology;

(e) To implement policies at the national and international levels to attract both public and private investment, domestic and foreign, that enhances knowledge, transfers technology on mutually agreed terms and raises productivity;

(f) To support the efforts of developing countries, individually and collectively, to harness new agricultural technologies in order to increase agricultural productivity through environmentally sustainable means;

2. *Recognizes* that science and technology, including information and communications technologies, are vital for the achievement of internationally agreed development goals, including the Millennium Development Goals, and for the full participation of developing countries in the global economy;

3. *Requests* the Commission on Science and Technology for Development to provide a forum within which to continue to assist the Economic and Social Council as the focal point in the system-wide follow-up to the outcomes of the World Summit on the Information Society[2] and to address within its mandate, in accordance with Council resolution 2006/46, the special needs of developing countries in areas such as agriculture, rural development, information and communications technologies and environmental management;

4. *Encourages* the United Nations Conference on Trade and Development, in collaboration with relevant partners, to continue to undertake science, technology and innovation policy reviews, with a view to assisting developing countries and countries with economies in transition in identifying the measures that are needed to integrate science, technology and innovation policies into their national development strategies;

5. *Encourages* the United Nations Conference on Trade and Development and other relevant organizations to assist developing countries in their efforts to integrate science, technology and innovation policies in national development strategies;

6. *Encourages* Governments to strengthen and foster investment in research and development for environmentally sound technologies and to promote the involvement of the business and financial sectors in the development of those technologies, and invites the international community to support those efforts;

7. *Encourages* existing arrangements and the further promotion of regional, subregional and interregional joint research and development projects by, where feasible, mobilizing existing scientific and research and development resources and by networking sophisticated scientific facilities and research equipment;

8. *Encourages* the international community to continue to facilitate, in view of the difference in level of development between countries, an adequate diffusion of scientific and technical knowledge and transfer of, access to and acquisition of technology for developing countries, under fair, transparent and mutually agreed terms, in a manner conducive to social and economic welfare for the benefit of society;

9. *Calls for* continued collaboration between United Nations entities and other international organizations, civil society and the private sector in implementing the outcomes of the World Summit on the Information Society, with a view to putting the potential of information and communications technologies at the service of development through policy research on the digital divide and on new challenges of the information society, as well as technical assistance activities, involving multi-stakeholder partnerships;

10. *Requests* the Secretary-General to submit to the General Assembly at its sixty-sixth session a report on the implementation of the present resolution and recommendations for future follow-up, including lessons learned in integrating science, technology and innovation policies into national development strategies.